Washington Administrative Code* requires state and local health departments to maintain case report information in a confidential manner.

The Department of Health recommends that local health departments and contractors have written policies and procedures governing the collection, storage, use, and disposal of confidential information. All staff should understand and abide by these polices.

Security and confidentiality training should be provided to all staff, and this training should be updated routinely. Security and confidentiality protections should be monitored on an ongoing basis.

All staff should sign formal agreements of confidentiality, acknowledging their personal responsibilities to protect identifying information from disclosure.

Breaches of confidential information should be thoroughly investigated and sanctions imposed when appropriate.

*WAC 246-100-016, WAC 246-100-036, WAC 246-100-091

Every individual with access to confidential information must take personal responsibility for its protection.

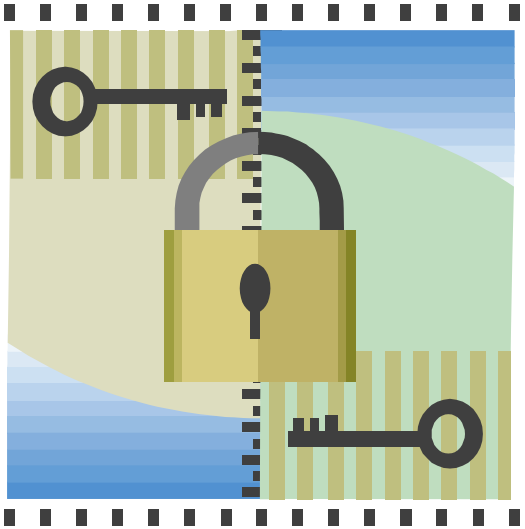
Following the basic principles of health care providers, which respect the human dignity and confidentiality of patients, Washington State law prohibits individuals who have knowledge of a person with a sexually transmitted disease (including HIV/AIDS) from disclosing the identity of the person or releasing information, except as specified in the Revised Code of Washington (RCW 70.24.105).

Violation of any provision of RCW 70.24 is a gross misdemeanor punishable by imprisonment for up to one year (RCW 9.92.020, and RCW 9A.20.021). In addition, violation may result in civil liability of up to $10,000 for reckless or intentional breech.

Persons who violate RCW 70.24 may be subject to both criminal and civil prosecution. Maximum penalities in civil lawsuits, where disclosure of confidential information results in loss of a job, housing, or other forms of injurious discrimination, have yet to be determined.

Washington State Department of Health
Infectious Disease and Reproductive Health
Olympia WA

Safeguarding



Confidential Information

Disease surveillance is a core public health function that depends upon trust.

Reporting cases of diseases and conditions of public health significance is necessary to monitor trends in disease. It is also useful to target prevention activities, evaluate the effectiveness of prevention and treatment, and allocate resources appropriately.

Effective surveillance depends upon the public's trust and cooperation, so that individuals are not dissuaded from seeking care and providers are not deterred from reporting cases.

The state and local surveillance, prevention, and care service programs must collect, store, and use this information in a way that protects individual privacy and respects human rights.

The HIV/AIDS surveillance program of the Washington State Department of Health has strict confidentiality and security standards which can provide a model for other agencies and programs that collect confidential information.

Patient information must be maintained in a secure and controlled environment.

The physical security of case report information must be assured. For example, the Centers for Disease Control and Prevention (CDC) require that health departments conform to strict security standards as a condition of funding for HIV/AIDS surveillance activities. These HIV/AIDS security guidelines include the following:

- Keep surveillance data inside locked cabinets in locked rooms without windows.
- Minimize the number of staff who have access to personal identifiers.
- Define, in writing, who has access to case report information and under what conditions.
- Protect keys, passwords, and codes that allow access to case report data.
- Remove HIV-related terms from any FAX containing case-specific information.
- Code risk information and remove all identifiers if reports are taken from their official, secured location.

Washington State Department of Health
Infectious Disease and Reproductive Health
Olympia WA

Additional recommendations for protecting confidentiality include:

- Discuss patient information only where conversations cannot be overheard.
- Never leave computer workstations unattended when using confidential electronic information.
- During field activities, take only the minimum amount of identifying information required to complete a given task. Carry it in a locked briefcase.
- Do not transfer identifying information through electronic media, including email, without specific authorization.
- When electronic transfer of information is authorized, encrypt the data and use only secure data transfer systems.
- Mail identifying information only to authorized recipients, and mark correspondence "Confidential".
- Develop a records retention schedule, and destroy information when it is no longer needed.
- Dispose of confidential information so that it is not retrievable. Cross-shred paper documents and "wipe" electronic media.